What is claimed is:

1. A method for generating an identity-based ring signature by using bilinear pairings, in a cryptosystem that includes a user, a signer and a trusted authority, which comprises the steps of:

(a) at the trusted authority, generating a set of system parameters shared by the user and the signer and storing the set of system parameters in a memory of each of the user and the signer;

(b) at the trusted authority, generating a public key and a private key for the user and the signer by using the set of system parameters, thereby transmitting the generated public and the private keys to the user and the signer through a secure channel, respectively;

(c) at the user, concealing content of a message and requesting a ring signature for the content-concealed message to the signer;

(d) at the signer, producing the ring signature based on identity (ID) of the user, thereby forming an ID-based ring signature for the content-concealed message; and

(e) at the user, verifying validity of the ID-based ring signature.

2. The method of claim 1, wherein the step (a) includes the steps of:

(a1) introducing a cyclic group G of an order q by means of a generator P, wherein the cyclic group G is an elliptic or hyper-elliptic curve Jacobian;

(a2) producing a multiplicative cyclic group V of the order q by using a bilinear pairing e expressed as the following Equation:

$$e: G \times G \rightarrow V$$

(a3) determining cryptographic hash functions

$$H: \{0,1\}^* \rightarrow Z_q^* \text{ and } H_1: \{0,1\}^* \rightarrow G;$$

wherein Z_q^* is a multiplicative cyclic group corresponding to V; and

(a4) selecting a master key s of the trusted authority and preparing a public key P_{pub} of the trusted authority by using the master key s and the generator P by using the following Equation

$$P_{pub} = s \cdot P.$$

3. The method of claim 2, wherein the set of system parameters has G, q, P_{pub}, P, H and H_1.

4. The method of claim 3, wherein the public key Q_{IDi} and the private key S_{IDi} of the user are stored in a memory of the user, which are defined by using the following Equations:

$$Q_{IDi} = H_1(ID_i) \text{ and } S_{IDi} = s \cdot Q_{IDi}$$

where ID_i is the user's identity, i being a user index which

is an integer ranging from 1 to n.

5. The method of claim 4, wherein the step (d) includes the steps of:

(d1) selecting an ID list L, wherein L is a set of identities of users;

(d2) extracting a random element A of the cyclic group G, thereby computing an initial signature value by using the ID list L;

(d3) choosing a random value of the cyclic group, thereby computing additional signature values by using the ID list L;

(d4) generating a ring signature value by using the private key of the signer;

(d5) forming a ring of ring signature values by selecting zero as a glue value of the additional signature values; and

(d6) storing in a memory of the user the ID-based ring signature of n+1 ring signature values.

6. The method of claim 5, wherein, at the signer, the initial signature value, c_{k+1}, is computed by using the following Equation:

$$c_{k+1} = H(L \parallel m \parallel e(A, P)),$$

wherein k is a signer index and m is the content-concealed message.

7. The method of claim 6, wherein an additional signature value is computed by using the following Equation:

$$c_{i+1} = H(L \parallel m \parallel e(T_i, P)\ e(c_i\ H_1(ID_i), P_{pub}))$$

for "i" corresponding to one of values of all modulo n (k+1, ···, n-1, 0, 1 and k-1), and then stored in a memory of the signer wherein T_i is the random value of the cyclic group G.

8. The method of claim 7, wherein the ring signature value, T_k, is calculated by using the following Equation:

$$T_k = A - c_k\ S_{IDk};$$

and stored in a memory of the signer.

9. The method of claim 8, wherein the ID-based ring signature is a sequence $(c_0, T_0, T_1, \cdots, T_{n-1})$, which is stored in a memory of the user.

10. The method of claim 9, wherein the validity of the ID-based ring signature is determined by using the following Equations:

$$c_{k+1} = H(L \parallel m \parallel e(A, P))$$

$$c_{k+2} = H(L \parallel m \parallel e(T_{k+1}, P)\ e(c_{k+1}\ H_1(ID_{k+1}), P_{pub}))$$

$$\vdots \qquad\qquad \vdots$$

$$c_n = H(L \parallel m \parallel e(T_{n-1}, P)\ e(c_{n-1}\ H_1(ID_{n-1}), P_{pub}))$$

$$c_1 = H(L \parallel m \parallel e(T_0, P)\ e(c_0\ H_1(ID_0), P_{pub}))$$

$$c_2 = H(L \parallel m \parallel e(T_1, P)\ e(c_1\ H_1(ID_1), P_{pub}))$$

$$\vdots \qquad\qquad \vdots$$

$$c_k = H(\, L \,\|\, m \,\|\, e(T_{k-1},\, P)\; e(c_{k-1}\; H_1(ID_{k-1}),\; P_{pub}))$$

wherein if i=0, 1,$\cdots$,n-1 and $c_n=c_0$, then the ID-based ring signature is determined to be valid; and if otherwise, the ID-based ring signature is rejected.

11. An apparatus for generating an identity-based ring signature by using bilinear pairings, comprising:

a trusted authority;

a user; and

a signer,

wherein the apparatus performs the steps of:

at the trusted authority, generating a set of system parameters shared by the user and the signer and storing the set of system parameters in a memory of each of the user and the signer;

at the trusted authority, generating a public key and a private key for the user and the signer by using the set of system parameters, thereby transmitting the generated public and the private keys to the user and the signer through a secure channel, respectively;

at the user, concealing content of a message and requesting a ring signature for the content-concealed message to the signer;

at the signer, producing the ring signature based on identity (ID) of the user, thereby forming an ID-based ring

signature for the content-concealed message; and

at the user, verifying validity of the ID-based ring signature.

12. The apparatus of claim 11, wherein the system parameters includes:

a cyclic group G;

G's order q;

G's generator P;

the trusted authority's public key P_{pub} described by $P_{pub} = s \cdot P$, where s is the master key; and

hash functions H and H_1 described by $H: \{0,1\}^* \rightarrow Z_q^*$ and $H_1: \{0,1\}^* \rightarrow G$, where Z_q^* is a cyclic multiplicative group, wherein the bilinear pairings e are defined by $e: G \times G \rightarrow V$, where V is a cyclic multiplicative group of the order q and uses cyclic multiplicative group Z_q^*,

the user's public key Q_{IDi} is described by $Q_{IDi} = H_1(ID_i)$, where ID_i is the user's identity, i being a user index which is an integer ranging from 1 to n,

the user's private key S_{IDi} is described by $S_{IDi} = s \cdot Q_{IDi}$,

the initial signature value is computed by $c_{k+1} = H(L \| m \| e(A, P))$, where k is a signer index, L is a set of identities of users, m is a content-concealed message to be ring-signed and A is a random element of the cyclic group G,

the additional signature values are generated by $c_{i+1} =$

$H(L \| m \| e(T_i, P)\ e(c_i\ H_1(ID_i), P_{pub}))$, for "i" corresponding to one of values of all modulo n (k+1, $\cdots$, n-1, 0, 1, k-1), where T_i is a random value of the cyclic group G,

the ID-based ring signature value, T_k, is calculated by

$T_k = A - c_k\ S_{IDk}$,

the ID-based ring signature is obtained in a form of a sequence $(c_0, T_0, T_1, \cdots, T_{n-1})$, and

the validity of the ID-based ring signature is determined by means of the following Equations:

$$c_{k+1} = H(L \| m \| e(A, P))$$

$$c_{k+2} = H(L \| m \| e(T_{k+1}, P)\ e(c_{k+1}\ H_1(ID_{k+1}), P_{pub}))$$

$$\vdots \qquad\qquad \vdots$$

$$c_n = H(L \| m \| e(T_{n-1}, P)\ e(c_{n-1}\ H_1(ID_{n-1}), P_{pub}))$$

$$c_1 = H(L \| m \| e(T_0, P)\ e(c_0\ H_1(ID_0), P_{pub}))$$

$$c_2 = H(L \| m \| e(T_1, P)\ e(c_1\ H_1(ID_1), P_{pub}))$$

$$\vdots \qquad\qquad \vdots$$

$$c_k = H(L \| m \| e(T_{k-1}, P)\ e(c_{k-1}\ H_1(ID_{k-1}), P_{pub}))$$

wherein if i=0, 1, $\cdots$, n-1 and $c_n=c_0$, then the ID-based ring signature is accepted to be valid; and if otherwise, the ID-based ring signature is rejected.